(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102349076 B
(45)授权公告日 2016.08.10

(21)申请号 201080011433.7

(22)申请日 2010.01.14

(30)优先权数据
12/355,063 2009.01.16 US

(85)PCT国际申请进入国家阶段日
2011.09.09

(86)PCT国际申请的申请数据
PCT/IB2010/000067 2010.01.14

(87)PCT国际申请的公布数据
WO2010/082123 EN 2010.07.22

(73)专利权人 诺基亚技术有限公司
地址 芬兰埃斯波

(72)发明人 J·A·阿尔韦 J-P·卢玛

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 酆迅

(51)Int.Cl.
G06F 21/10(2013.01)

(56)对比文件
WO 03/083627 A2,2003.10.09,说明书第1,3-5页,附图1-2.
US 2003/0076955 A1,2003.04.24,全文.
CN 1748422 A,2006.03.15,全文.

审查员 姚楠

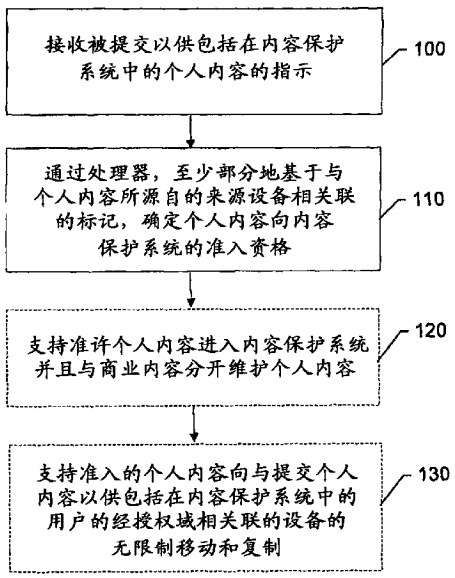
权利要求书2页 说明书10页 附图3页

(54)发明名称

用于保护个人内容的内容保护系统的方法、装置和计算机程序产品

(57)摘要

一种用于提供保护个人内容的内容保护系统的装置，其可以包括处理器，该处理器配置用于接收被提交以供包括在内容保护系统中的个人内容的指示，以及至少部分地基于与个人内容所源自的来源设备相关联的标记确定个人内容向内容保护系统的准入资格。还提供了相应的方法和计算机程序产品。



CN 102349076 B

1.一种用于提供保护个人内容的内容保护系统的方法，包括：

接收被提交以供包括在内容保护系统中的个人内容的指示；以及

通过处理器至少部分地基于与所述个人内容所源自的来源设备相关联的标记确定所述个人内容向所述内容保护系统的准入资格，

所述标记验证所述个人内容来自可信非商业源；以及

支持准许所述个人内容进入所述内容保护系统以及与商业内容分开维护所述个人内容；

其中所述内容保护系统适于存储所述个人内容和所述商业内容。

2.根据权利要求1所述的方法，其中确定所述个人内容的准入资格包括确定所述个人内容是否包括使用状态，所述使用状态限定针对不与用户的经授权域相关联的设备不允许对所述个人内容的无限制复制，所述用户是提交所述个人内容以供包括在所述内容保护系统中的用户。

3.根据权利要求1所述的方法，还包括支持准入的个人内容向设备的无限制移动和复制，所述设备与用户的经授权域相关联，所述用户是提交所述个人内容以供包括在所述内容保护系统中的用户。

4.根据权利要求1所述的方法，其中确定所述个人内容的准入资格包括确定所述个人内容是否包括指示所述来源设备的水印。

5.根据权利要求1至4中任意一项所述的方法，其中确定所述个人内容的准入资格包括基于关于所述个人内容是否包括与已知商业内容相关联的数字指纹的确定来确定准入资格。

6.一种用于提供保护个人内容的内容保护系统的装置，包括：

用于接收被提交以供包括在内容保护系统中的个人内容的指示的装置；以及

用于至少部分地基于与所述个人内容所源自的来源设备相关联的标记确定所述个人内容向所述内容保护系统的准入资格的装置，

所述标记验证所述个人内容来自可信非商业源；以及

用于支持准许所述个人内容进入所述内容保护系统以及与商业内容分开维护所述个人内容的装置；

其中所述内容保护系统适于存储所述个人内容和所述商业内容。

7.根据权利要求6所述的装置，其中确定所述个人内容的准入资格包括用于确定所述个人内容是否包括使用状态的装置，所述使用状态限定针对不与用户的经授权域相关联的设备不允许对所述个人内容的无限制复制，所述用户是提交所述个人内容以供包括在所述内容保护系统中的用户。

8.根据权利要求6所述的装置，还包括用于支持准入的个人内容向设备的无限制移动和复制的装置，所述设备与用户的经授权域相关联，所述用户是提交所述个人内容以供包括在所述内容保护系统中的用户。

9.根据权利要求6所述的装置，其中确定所述个人内容的准入资格包括用于确定所述个人内容是否包括指示所述来源设备的水印的装置。

10.根据权利要求6至9中任意一项所述的装置，其中确定所述个人内容的准入资格包括用于基于关于所述个人内容是否包括与已知商业内容相关联的数字指纹的确定来确定

准入资格的装置。

用于保护个人内容的内容保护系统的方法、装置和计算机程序产品

技术领域

[0001] 本发明的实施方式总体上涉及内容共享技术，并且更具体地，涉及用于提供保护个人内容的内容保护系统的装置、方法和计算机程序产品。

背景技术

[0002] 现代通信时代已经引起了有线和无线网络的极大扩张。计算机网络、电视网络和电话网络正在经历由消费者需求所激起的空前的技术扩展。无线和移动组网技术已经满足了相关的消费者需求，并提供了对于信息传递的更多灵活性和直接性。

[0003] 当前和未来的组网技术通过扩展移动电子设备的能力而持续促进对用户的信息传递容易性以及便利性。存在增加信息传递容易性的要求的一个领域涉及在多个设备之间以及潜在地在多个用户之间共享信息。在此方面，鉴于现代电子设备创建和修改内容、以及分发或者共享内容的能力，此类设备的用户变为媒体内容的制造者和多产用户(prolific user)很常见。已经开发了网络和服务来支持用户向网络内的不同点移动已创建的内容。

[0004] 为了补充用于分发和共享个人内容的机制，还开发了机制来提供商业内容的分发。为了防止对商业内容的未授权使用或复制，已经存在针对有时采取数字权利管理(DRM)形式的内容保护的增加的需求。已经开发了例如DVB CPCM(数字视频广播内容保护和复制管理)之类的内容保护系统，以提供防止对商业内容的不适当使用的保护。DVB CPCM根据与商业数字内容相关联的特定使用规则，自获取到系统中直到最终消费(或者从该系统输出)，管理向消费者产品和家庭网络递送的商业数字内容的使用。商业数字内容的示例可以包括所有类型的内容，诸如音频、视频以及相关联的应用和数据，其中任一均可以经由广播服务、基于因特网的服务、封包媒体以及移动服务等进行接收。诸如DVB CPCM之类的示例性内容保护系统可以提供规范，以促进内容在由用于家庭组网和远程访问两者的联网消费者设备获取之后的互操作性。因此，典型的内容保护系统可以定义信令及技术遵从标准以保证互操作性。

[0005] 鉴于设计用于提供针对商业内容的保护的内容保护系统可以向由该系统呈现的内容添加某些合法性的暗示，经由内容保护系统提供内容可能是某些人可能希望通过其向其他人提供个人内容的期望机制。然而，在某些情况下合法性的暗示可能被误用。例如，被非法复制或者获取的非法出售的电影、音乐以及其他内容可以通过将此类内容上传到内容保护系统并且使该内容可通过内容保护系统免费获得而经历“内容清洗(content laundering)”。为了防止使非法内容看似是合法内容的内容清洗，许多内容提供者不愿接受任何个人的或者用户创建的内容进入内容保护系统中。

[0006] 尽管有上述问题，仍存在个人内容可以从经由内容保护系统保护而获益的合法原因。例如，用户可能希望向参加聚会的人发送出自该聚会的照片，但是可能不希望允许这些人进一步向他们的朋友分发该内容或者在因特网上发布该内容。因此，期望提供关于处理个人内容的改进的内容保护系统。

发明内容

[0007] 因此，提供了可以提供用于处理个人内容的内容保护系统的方法、装置和计算机程序产品。因此，例如，可以支持通过内容保护系统向其他用户分发个人内容，该分发具有此类用户可以关于所分发的内容而进行的活动上的限制。此外，可以在提供内容以供分发的用户的不同设备之间自由移动该内容(以及可能的复制)。

[0008] 在一个示例性实施方式中，提供了提供用于保护个人内容的内容保护系统的方法。该方法可以包括接收被提交以供包括在内容保护系统中的个人内容的指示，以及至少部分地基于与个人内容所源自的来源设备相关联的标记确定个人内容向内容保护系统的准入资格。

[0009] 在另一示例性实施方式中，提供了用于提供用于保护个人内容的内容保护系统的计算机程序产品。该计算机程序产品包括至少一个计算机可读存储介质，该计算机可读存储介质具有存储在其中的计算机可执行程序代码指令。该计算机可执行程序代码指令可以包括用于以下的程序代码指令：接收被提交以供包括在内容保护系统中的个人内容的指示，以及至少部分地基于与个人内容所源自的来源设备相关联的标记确定个人内容向内容保护系统的准入资格。

[0010] 在又一示例性实施方式中，提供了用于提供用于保护个人内容的内容保护系统的装置。该装置可以包括处理器。该处理器可以配置用于接收被提交以供包括在内容保护系统中的个人内容的指示，以及至少部分地基于与个人内容所源自的来源设备相关联的标记确定个人内容向内容保护系统的准入资格。

[0011] 在一个示例性实施方式中，提供了用于提供用于保护个人内容的内容保护系统的装置。该装置可以包括用于接收被提交以供包括在内容保护系统中的个人内容的指示的装置，以及用于至少部分地基于与个人内容所源自的来源设备相关联的标记确定个人内容向内容保护系统的准入资格的装置。

[0012] 相应地，本发明的实施方式可以支持关于在多个设备上共享内容的改进的能力。

附图说明

[0013] 已经如此概括地描述了本发明，现在将参考附图，附图不必按比例绘制，并且其中：

[0014] 图1是根据本发明的示例性实施方式的系统的示意性框图；

[0015] 图2是根据本发明的示例性实施方式的用于提供用于个人内容保护的内容保护系统的装置的示意性框图；以及

[0016] 图3是按照根据本发明的示例性实施方式的用于提供用于保护个人内容的内容保护系统的示例性方法的流程图。

具体实施方式

[0017] 现在将在下文中参考附图更充分地描述本发明的某些实施方式，在附图中示出了本发明的某些但非全部实施方式。事实上，本发明的各种实施方式可以体现为许多不同形式，并且不应当被解释为限制到在此阐明的实施方式。贯穿全文，类似的参考号指代类似的

元素。如在此使用的，术语“数据”、“内容”、“信息”以及类似术语可以互换使用以指代能够根据本发明的实施方式被传递、接收和/或存储的数据。此外，如在此使用的，术语“示例性”并非被提供用于表达任何定性评价，而是反之仅仅表达示例的说明。因此，对任何此类术语的使用均不应当被用以限制本发明的实施方式的精神和范围。

[0018] 如上所述，本发明的实施方式可以在方法、装置和计算机程序产品中加以利用，以便提供具有在提供个人内容的同时解决内容提供者对于内容清洗可能性的担心的能力的内容保护系统。在此方面，例如，本发明的实施方式可以规定在满足某些条件时将个人内容引入内容保护系统中。用于将个人内容引入内容保护系统中的一个示例条件可以包括来源认证。在此方面，如果待引入系统中的内容源自个人内容的经认证来源，则可以允许该内容进入系统中。另一示例条件可以包括复制限制。在此方面，例如，与待引入系统中的内容相关联的使用状态可以不允许对内容的无限制复制(至少针对不与证明该内容的用户的经授权域相关联的设备)，以便消除内容清洗者(launderer)的典型动机。作为又一示例条件，当在内容保护系统中时，可以将个人内容与商业内容隔离。对个人内容与商业内容的隔离可以促进管理具有略为不同的使用规则的个人内容以及对现有内容保护系统使用状态的潜在扩展，以支持提供个人内容保护。

[0019] 因此，个人内容可以与内容保护系统相关联地被创建、复制、修改和分发，以及从该系统所给予的保护中获益。然而，尽管本发明的实施方式可以支持用户对个人内容向其他用户的分发加以限制，但是可以支持用户的经授权域(authorized domain)(其可以包括被注册为属于该用户的该用户的个人拥有的设备(例如，媒体播放器、移动电话、膝上型计算机或者个人计算机(PC)、相机或者摄像机等))在设备之间自由地移动内容。

[0020] 图1图示了可以得益于本发明的实施方式的系统的框图。然而，应当理解，如被示出并且在以下描述的该系统仅仅是可以得益于本发明的实施方式的一个系统的说明，并且因此不应当被用作限制本发明的实施方式的范围。此外，虽然DVB CPCM被当作内容保护系统的一个示例，但应当理解，本发明的实施方式并非限于具有DVB CPCM的应用，而是也可以与其他内容保护系统结合使用。

[0021] 如图1中所示，根据本发明的示例实施方式的系统的实施方式可以包括用户终端10，其能够经由网络30与包括例如服务平台20的许多其他设备进行通信。服务平台20可以是服务器、服务器组(server bank)或者配置用于经由网络30提供一个或多个服务(例如，因特网服务)的其他计算机。在示例性实施方式中，服务平台20还可以提供内容管理、内容共享、内容获取以及与通信和媒体内容有关的其他服务等。诺基亚的Ovi套件是可以与服务平台20相关联的服务提供机制的示例。在某些情况中，服务平台20可以包括内容保护系统22、与内容保护系统22相关联或以其他方式与内容管理系统22功能性联合。内容保护系统22可以配置用于提供如在此描述的内容保护服务，以便支持关于引入内容保护系统22中的内容的DRM。内容保护系统22可以是诸如体现为配置用于执行如在此描述的内容保护系统22的相应功能的硬件、软件或者硬件和软件的组合的设备或者电路之类的任何装置。因此，例如在某些情况中，内容保护系统22可以体现为服务器、服务器组或者其他计算设备。内容保护系统22可以配置用于根据指定的规则提供内容的存储(在某些情况中，在商业或者个人内容分类的基础上被隔离)和分发。例如，可以仅将内容向经授权用户分发。

[0022] 在示例性实施方式中，可以采用内容保护代理24来筛选意在向内容保护系统22提

交的内容。在此方面，例如，内容保护代理24可以充当配置用于应用预定义规则和/或准则以便确定是否允许被提交用于包括在内容保护系统22中的内容进入内容保护系统22的网关或者访问控制机构。此外，如果所提交的内容由内容保护代理24选择以供包括在内容保护系统22中，则内容保护代理24可以定义可以应用于该内容的条件参数或者使用状态参数。使用状态参数可以关于管理内容的存储和/或分发的特定规则来向内容保护系统22做出指令。内容保护代理24可以是诸如体现为配置用于执行如在此描述的内容保护代理24的相应功能的硬件、软件或者硬件和软件的组合的设备或者电路之类的任何装置。在某些情况中，内容保护代理24可以被体现在内容保护系统22处，如图1中所示。然而，在备选实施方式中，内容保护代理24可以被体现在该系统中的另一设备处(例如，在服务平台20、用户终端10处等)。

[0023] 在本发明的某些实施方式中，该系统还可以包括一个或者多个附加设备，诸如个人计算机(PC)、服务器、网络硬盘、文件存储服务器等，它们能够与用户终端10通信并且可由服务平台20访问。在某些情况中，用户终端10可以是针对进入内容保护系统22(例如，经由内容保护代理24)的内容的获取点。因此，可以支持用户终端10直接向内容保护系统22提供内容。然而，在某些实施方式中，用户终端10可以配置用于经由采取内容保护代理24的形式的物理分离的获取点向内容保护系统22提供内容。获取点(例如，采取内容保护代理24的形式)可以是能够与一个或者多个用户终端进行通信以便将一个或多个用户终端所提交的内容提供给内容保护系统22的通信设备。因此，其自身可以体现为配置用于经由网络30与内容保护系统22进行通信的计算设备、服务器或其他通信设备，或者体现为计算设备、服务器或者其他通信设备的一部分的获取点可以是配置用于确定内容的来源是否为用于向内容保护系统22提交内容的经授权和/或可信设备的代理。

[0024] 用户终端10可以是多种类型的固定或者移动通信和/或计算设备的任意种类，这些设备是诸如便携式数字助理(PDA)、寻呼机、移动电视、移动电话、游戏设备、膝上型计算机、PC、相机、带摄像头的电话、录像机、音频/视频播放器、收音机、全球定位系统(GPS)设备，或者任何前述诸项的组合，以及利用本发明的实施方式的其他类型的语音和文本通信系统。

[0025] 网络30可以包括可以经由相应的有线和/或无线接口相互通信的各种不同节点、设备或者功能的聚集。因此，图1的图示应当被理解为该系统的某些元件的宽泛视图的示例，并且不是该系统或者网络30的总括性的或者详细的视图。虽然并未必要，但是在某些实施方式中，网络30可以能够支持按照多个第一代(1G)、第二代(2G)、2.5G、第三代(3G)、3.5G、3.9G、第四代(4G)移动通信协议、长期演进(LTE)等中的任何一种或者多种的通信。因此，网络30可以是蜂窝网络、移动网络和/或数据网络，诸如局域网(LAN)、城域网(MAN)和/或广域网(WAN)，例如因特网。相应地，其他设备(诸如处理元件(例如，个人计算机、服务器计算机等))可以包含在网络30中或者耦合到网络30。通过直接或者间接地将用户终端10和其他设备连接到网络30，可以支持用户终端10和/或其他设备例如根据包括超文本传输协议(HTTP)等的许多通信协议进行相互通信，从而分别实现移动终端10和其他设备的各种通信或者其他功能。因此，可以支持用户终端10和其他设备通过许多不同访问机制中的任何机制与网络30通信和/或相互通信。例如，可以支持移动访问机制(诸如宽带码分多址(W-CDMA)、CDMA2000、全球移动通信系统(GSM)、通用分组无线电业务(GPRS)等)以及无线访问

机制(诸如无线LAN(WLAN)、微波访问全球互联(WiMAX)、WiFi、超宽带(UWB)、Wibree技术等)以及固定访问机制(诸如数字用户线路(DSL)、电缆调制解调器、以太网等)。因此,例如,网络30可以是家庭网络或者提供本地连接的其他网络。

[0026] 在示例性实施方式中,服务平台20可以是诸如服务器或者其他处理元件之类的设备或者节点。服务平台20可以具有任何数量的功能或者与各种服务的关联。因此,例如,服务平台20可以是诸如与特定信息来源或者服务(例如,诺基亚的Ovi套件)相关联的专用服务器(或者服务器组)之类的平台,或者服务平台20可以是与一个或者多个其他功能或者服务相关联的后端服务器。因此,服务平台20代表用于多个不同服务或者信息来源的潜在主机。在某些实施方式中,服务平台20的功能由被配置成根据用于向通信设备的用户提供信息的已知技术进行操作的硬件和/或软件组件来提供。然而,至少某些由服务平台20提供的功能可以是根据本发明的实施方式提供的数据处理和/或服务提供功能。

[0027] 如在此使用的,术语“个人内容”可以指代包括非商业性质的音频、视频和/或媒体内容在内的内容。换言之,个人内容并非是为了交换金钱报酬而分发的。本发明的实施方式支持经由被授权提供个人内容的获取点(例如,内容保护代理24)将此类内容引入内容保护系统22中。在某些实施方式中,可以将获取点整合在用户终端10内。因此,例如,用户终端10可以代表配置用于创建内容(例如通过相机以及可能还通过麦克风)以及还向内容保护系统22提供所创建的内容的单个物理设备。通过鲁棒构建,根据本示例的用户终端10可以被配置用于防止来自其他的、未经授权的来源的数字内容经由获取点40被引入到内容保护系统22。

[0028] 在备选实施方式中,获取点可以不是用户终端10的一部分。因此,例如,用户终端10可以经由网络30(在某些情况中经由安全链路)连接到获取点。在这样的实施方式中,获取点可以配置用于确定所提交的内容的来源(例如,用户终端10)是否能够被明确地验证。在此方面,例如,获取点可以配置用于利用与来源相关联的数字证书作为用于验证个人内容的来源的工具。

[0029] 在另一备选实施方式中,用户终端10(例如,作为个人内容的可信来源)可以使用水印或者其他标识符标记内容,这明确地将内容标识为源自个人内容的可信来源。获取点可以配置用于寻找水印作为允许内容进入内容保护系统的条件。

[0030] 在本发明的又一备选实施方式中,获取点可以被实现为与特定用户账户相关联的可信内容共享服务(例如服务平台20)的一部分,并且因此是特定用户的经授权域的一部分。可以针对由用户向服务平台20的内容共享服务上传的内容的每个项目(或者随机地针对某些内容项目)计算诸如pHash(感知哈希算法)之类的数字指纹。可以将数字指纹与商业内容项目的已知指纹成对地进行比较。如果确定为精确的或者接近的匹配,则结果可以包括:阻止用户向获取点的当前上传以及可能的未来上传,和/或通知内容所有者。由于针对大量商业内容项目的哈希而检查每个由用户提供的内容剪辑的哈希可能是耗时的演进(evolution),并且消耗过多时间可能是不期望的,因此在某些实施方式中,可以将对哈希的检查作为在服务器侧上(例如在服务平台20)的后台作业完成而不引起对用户的与上传该内容有关的延迟。在某些实施方式中,可以仅仅在例如在随机采样的基础上提交的内容的某些部分上完成检查。此类随机检查仍然可以充当针对非法商业内容再分发企图的遏制因素。

[0031] 在某些情况中，分离的个人内容签名单元12可以连同现存的照片或视频捕捉/编辑设备而被包括或者以其他方式可被连同该设备使用，以使用用户的个人签名或者与用户相关联并且向用户的服务平台20登记的某些其他标记对内容加标记。内容签名单元12可以是诸如体现为配置用于执行如在此描述的内容签名单元12的相应功能的硬件、软件或者硬件和软件的组合的设备或者电路之类的任何装置。虽然在图1中连同用户终端10示出，但内容签名系统12可以备选地位于用户家中的另一位置、与服务平台20位于同一地点或者位于可信第三方的场所。因此，用户可以向与服务平台20相关联的内容共享服务提供者登记他们的相应联系信息。所登记的联系信息可以与用户的相机或者其他内容创建设备的签名或者其他标记相关联，或者可以与用户的个人签名相关联。在某些情况下，联系信息可以仅可由官方(authority)访问，例如，使用内容共享服务提供者的数据库中的密钥托管加密，以协助对非法商业内容再分发的调查。

[0032] 用户或者用户的内容创建设备(例如，相机)的签名或者其他标记也可以充当数字指纹，以阻止使用相机从某些其他设备的屏幕捕捉电影或者其他商业内容的企图。在某些情况中，指纹可能允许追踪回内容的来源，以由此阻止某些合法活动，例如，在公共内容共享服务(例如YouTube)上发布警察暴行视频。因此，按照以下方式使用指纹识别可以是有利的，即使得可以证明某个视频来自相应的某个相机，但不能(至少在没有适当授权的情况下)比较两个视频以及证明它们来自相同相机。实现此方式的一种途径可以是在签名块中包括随机数并且使用与内容共享服务提供者相关联的公共密钥对该签名块加密。因此，只有内容共享服务提供者可以使用相应的私人密钥对签名块解密，在此之后可以进行签名检查。

[0033] 在示例性实施方式中，对签名块进行加密可以由实体E实现，其可以是例如产生个人内容的设备或者单独的内容签名单元。以下描述用于创建签名块的示例性过程。然而，应当理解，在此描述的过程仅仅是一个示例而非限制本发明的实施方式。在一个示例中，最初可以计算媒体内容上的哈希H(M)。可以使用对称加密(例如，$E_K(H(M),ID)$)，用唯一会话密钥K对该哈希和设备ID加密。可以使用内容共享服务提供者的公共密钥$E_S(K)$对会话密钥加密。签名块可以是经加密会话密钥和对称加密的结果的拼接(例如，$SB(M)=E_S(K),E_K(H(M),ID)$)。在示例性实施方式中，作为逆过程，共享服务提供者可以使用其私人密钥以获得签名块的会话密钥K，$K=D_S(E_S(K))$。共享服务提供者还可以或者备选地能够使用会话密钥K以获得设备ID，连同使签名块与内容相互关联的哈希(例如，$H(M),ID=D_K(E_K(H(M),ID))$)。关于以上方程式，ID项指代产生个人内容的设备的唯一标识符。M项指代内容，诸如视频、音频或者相片。SB(M)项指代用于内容M的签名块。K项指代唯一会话密钥。$E_K()$项指代使用密钥K对消息进行的加密。$E_S()$项指代使用共享服务提供者的公共密钥对消息进行的加密。$D_S()$项指代使用共享服务提供者的相应的私人密钥对消息进行的解密。H()项指代使用哈希函数(例如SHA或者MD5)对摘要进行的计算。

[0034] 用于保护个人内容的一个示例性用例可以包括提供用于向不完全可信的朋友和熟人给予图片的单一副本的支持，但阻止该单一副本的接收者制作另外的副本。在此类情况中，本发明的实施方式可以支持媒体内容的提供者向提供者的经授权域自由复制该媒体内容，但可以将该媒体内容标记为“不再复制”或者以某些其他适合的方式阻止经授权域之外的复制。由于当前的内容保护系统(例如当前的DVBCPCM规范)不包括用于限制超出经授

权域的复制的使用状态，因此本发明的实施方式可以提供使用状态扩展以支持此类限制。

[0035] 作为备选，可以向内容共享网站(例如，Ovi)上传内容，该网站可以提供访问控制以限制内容观看特权所扩展到的当事方。内容可以具有使用状态集合以支持在内容保护系统内的观看(例如，VCPCM＝在整个CPCM系统内可观看)，但限制内容向经授权域内的移动和/或复制(例如，MAD＝在经授权域内可移动)。在示例性实施方式中，在内容保护代理24处按照用于使用本发明的实施方式的装置(例如，图2的装置50)的形式实现的软件、硬件或者软件和硬件的组合可以实现用于管理针对全部用户的内容分发的单个内容管理代理24或者针对每个已登记用户的独立的内容管理实体。因此，在某些实施方式中，可以针对能够上传内容的每个已登记用户实例化采取内容保护和内容管理机构或者设备形式的内容保护代理24的单独实例。继而，可以在使内容可以被上传前将每个实例加入到相应的已登记用户的经授权域。在某些实施方式中，访问控制可以基于密码，并且用于观看而利用的密码可以不同于用于将内容保护代理24的某个用户实例加入到他的/她的经授权域而利用的密码。在示例性实施方式中，内容保护代理24可以配置用于记录对指示个人内容的可信来源的信息或以其他方式具有对该信息的访问权。在某些情况中，某些种类的设备可以被认为是个人内容的可信来源。可信来源可以包括相机(例如，照相机或者摄像机)、乐器或者播放器以及可以生成媒体内容的其他设备(可能还包括麦克风)。在某些情况中，可信来源(例如相机)可以是另一设备内的设备(例如在移动电话内设置的相机)或者整合部分。因此，如果内容保护系统获取点(例如内容保护代理24)能够明确地标识内容源自个人内容的此类可信来源，则获取点可以允许内容进入内容保护系统22。

[0036] 由获取点(例如内容保护代理24)向个人内容应用的使用状态可以在某种程度上受到用户控制，但是可以存在由获取点执行的手段以限定使用状态不允许无限制复制。换言之，内容保护代理24可以限定对关于被提交用于包括在内容保护系统22中的内容的可允许动作进行限定的使用参数。在此方面，例如，对被提交用于包括在内容保护系统22中的内容的复制可以被限制到提交该内容的用户的经授权域或者本地环境。在备选实施方式中，示例性使用参数或者使用状态可以限定对被提交用于包括在内容保护系统22中的内容所制作的副本数量的数量限制。在某些情况中，也可以提供使用状态的组合。用于决定对基于可以限制所提交内容的共享的使用参数的布置的所提交内容的接受的一个示例性基本原理在于，如果用户不希望该内容具有某种类型的复制限制，则没有理由首先将该内容置于内容保护系统22中。自然地，总是允许用户在内容保护系统22之外保有个人内容的无保护副本。然而，对于向内容保护系统22提交的内容，限制复制的策略可以减少内容清洗威胁，这是因为该限制将阻止经由内容保护系统22非法再分发商业内容的企图。

[0037] 为了进一步减小使用可信设备(甚至降低质量地(例如通过使用摄像机当在电影院中播放电影时摄录电影))对商业内容清洗的风险，可以使用如上述pHash机制之类的数字签名技术以检测由特定用户向系统上传的任何商业内容。在某些情况中，可以通过把由内容保护系统22支持的符合以及鲁棒制度(C&R制度)用于个人内容而在个人内容的整个生命周期中保持将个人内容同商业内容分离。作为示例，DVB CPCM内容许可可以具有被称为“C&R制度掩码”的字段，其每个比特信令该内容是否在C&R制度下可用。同样地，CPCM实例证书可以具有被称为C_and_R_regime_mask的匹配字段，其指示CPCM实例(或设备)支持哪个C&R制度的内容。

[0038] 在示例性实施方式中，提供了可以在执行本发明的示例性实施方式的设备处使用的装置50。装置50可以体现为例如托管、包含、控制或以其他方式包括内容保护代理24的任何设备。因此，当内容保护代理24被体现在用户终端10时，装置50可以是用户终端10，或者当内容保护代理24被体现在以下实体中的相应的一个时，该装置可以是服务平台20或者内容保护系统22的服务器或者其他设备，或者是网络30自身。然而，实施方式也可以体现在多种其他设备上，诸如装置50的实例可以体现在客户端侧和服务器侧设备两者上。因此，将会概括地描述装置50，以便对客户端侧和服务器侧设备具有宽泛的应用。因此，图2的装置50仅仅是示例并且可以包括比图2中所示出的组件更多(或者在某些情况中，更少)的组件。

[0039] 现在参照图2，其提供了用于使用内容筛选以供将此类内容提交到内容保护系统内的装置。装置50可以包括处理器70、用户接口72、通信接口74和存储器设备76，或者以其他方式与它们通信。存储器设备76可以包括例如易失性和/或非易失性存储器。存储器设备76可以配置用于存储信息、数据、文件、应用、指令等。例如，存储器设备76可以配置用于缓存输入数据以供由处理器70处理。附加地或者备选地，存储器设备76可以配置用于存储指令以供由处理器70执行。作为又一备选，存储器设备76可以是存储信息和/或媒体内容的多个数据库或者存储位置之一。

[0040] 处理器70可以体现为多种不同方式。例如，处理器70可以体现为各种处理装置，诸如处理元件、协处理器、控制器，或者各种其他处理设备，包括诸如ASIC(专用集成电路)、FPGA(现场可编程门阵列)、硬件加速器等集成电路。在示例性实施方式中，处理器70可以配置用于执行存储在存储器设备76中或者以其他方式可由处理器70访问的指令。因此，无论是由硬件或软件方法或由它们的组合配置，处理器70均可以代表能够在相应地配置的情况下执行根据本发明的实施方式的操作的实体。因此，例如，当处理器70体现为ASIC、FPGA等时，处理器70可以是用于实施在此描述的操作的特别配置的硬件。备选地，作为另一示例，当处理器70体现为软件指令的执行器时，该指令可以特别地配置处理器70(如果不是用于由指令提供的特定配置，则其可以是通用处理元件)以执行在此描述的算法和操作。然而，在某些情况中，处理器70可以是通过由用于执行在此描述的算法和操作的指令对处理器70进一步配置而适合于使用本发明的实施方式的特定设备(例如移动终端)的处理器。

[0041] 与此同时，通信接口74可以是诸如体现为配置用于从网络和/或与装置50通信的任何其他设备或者模块接收数据和/或向它们传递数据的硬件、软件或者硬件和软件的组合的设备或者电路之类的任何装置。在此方面，通信接口74可以包括例如用于支持使用无线通信网络(例如网络30)进行通信的天线(或者多个天线)以及支持硬件和/或软件。在固定环境中，通信接口74可以备选地或者还支持有线通信。因此，通信接口74可以包括通信调制解调器和/或其他硬件/软件以支持经由电缆、数字用户线路(DSL)、通用串行总线(USB)、以太网、高清晰度多媒体接口(HDMI)或者其他机构进行通信。此外，通信接口74可以包括硬件和/或软件以支持诸如蓝牙、红外线、UWB、WiFi之类的通信机制，其正越来越多地连同提供家庭连接解决方案而被使用。

[0042] 用户接口72可以与处理器70通信以接收在用户接口72处的用户输入的指示和/或向用户提供可听、可视或者机械的或者其他输出。因此，用户接口72可以包括例如键盘、鼠标、控制杆、显示器、触摸屏、麦克风、扬声器或者其他输入/输出机构。在装置被体现为服务器或者某些其他网络设备的示例性实施方式中，用户接口72可以是受限的、位于远程的或

者被除去。

[0043] 在示例性实施方式中，处理器70可以体现为、包括或以其他方式控制内容筛选器78。根据某些实施方式，内容筛选器78是诸如体现为配置用于执行关于被提交以供包括在内容保护系统22中的媒体内容的内容筛选功能的硬件、软件或者硬件和软件的组合的设备或者电路之类的任何装置。在此方面，例如，内容筛选器78配置用于接收被提交以供包括在内容保护系统22中的个人内容的指示并且确定是否允许此类内容包括在内容保护系统22内。在示例性实施方式中，内容筛选器78可以配置用于至少部分地基于与个人内容所源自的来源设备相关联的标记来确定个人内容向内容保护系统22的准入资格。换言之，例如，如果来源设备是经授权来源(例如与由服务平台20提供的服务的已登记用户相关联的已知设备)，则可以允许个人内容进入内容保护系统。

[0044] 在某些实施方式中，内容筛选器78可以配置用于以将个人内容与商业内容分开维护的方式支持个人内容进入内容保护系统22。因此，可以使用独立的存储位置或者可以使用机制以在单个存储位置(例如存储器设备76)内区分个人内容和商业内容。

[0045] 在示例性实施方式中，内容筛选器78还可以配置用于例如基于与个人内容相关联的使用状态或者使用参数应用规则，以在允许个人内容进入内容保护系统22之后管理个人内容的使用、移动和/或复制。由内容筛选器78应用的规则可以限定例如可以向与提交个人内容以供包括在内容保护系统中的用户的经授权域相关联的设备完成对准入的个人内容的无限制移动和复制。然而，该规则可能还限定对于不与经授权域相关联的设备不允许对个人内容进行无限制复制。在示例性实施方式中，内容筛选器78可以配置用于在个人内容内检测标记，诸如确定个人内容是否包括指示来源设备的水印或者指示设备或者用户的签名。在某些情况中，内容筛选器78还可以配置用于确定个人内容是否包括与已知商业内容相关联的数字指纹，并且将个人内容的准入资格建立在个人内容的数字指纹与已知商业内容的数字指纹的比较的基础上。在某些情况中，可以基于全部或者部分(在某些情况中是随机部分)正被比较的内容的哈希或者感知哈希执行内容比较。

[0046] 因此，本发明的某些实施方式提供由内容保护系统提供的给予个人内容的保护的益处，同时挫败使用内容保护系统进行对商业内容的内容清洗的企图。

[0047] 图3是根据本发明的示例性实施方式的系统、方法和程序产品的流程图。应当理解，流程图的每个块或者步骤，以及流程图中块的组合，可以由诸如硬件、固件和/或包括一个或多个计算机程序指令的软件之类的各种手段实现。例如，以上描述的一个或多个过程可以由计算机程序指令体现。在此方面，在示例实施方式中，体现以上描述的过程的计算机程序指令由存储器设备(例如存储器设备76)存储并且由处理器(例如处理器70)执行。如将被领会的，任何此类计算机程序指令可以被加载到计算机或者其他可编程装置(即，硬件)上以产生机器，从而使得在计算机或者其他可编程装置上执行的指令创建用于实现在一个或多个流程图块或者步骤中指定的功能的装置。在某些实施方式中，计算机程序指令存储在计算机可读存储器中，该计算机可读存储器可以引导计算机或者其他可编程装置按照特定方式运行，从而使得存储在计算机可读存储器中的指令产生制品，该制品包括实现在一个或多个流程图块或者步骤中指定的功能的指令装置。计算机程序指令还可以被加载到计算机或者其他可编程装置上，以使得在该计算机或者其他可编程装置上执行一系列操作步骤，以产生由计算机实现的过程，从而使得在计算机或者其他可编程装置上执行的指令提

供用于实现在一个或多个流程图块或者步骤中指定的功能的步骤。

[0048] 因此，流程图的块或者步骤支持用于执行所指定功能的装置的组合、用于执行所指定功能的步骤的组合以及用于执行所指定功能的程序指令装置。还应当理解，流程图的一个或多个块或者步骤，以及流程图中的块或者步骤的组合，可以由执行所指定的功能或者步骤的基于专用硬件的计算机系统或者专用硬件和计算机指令的组合来实现。

[0049] 在此方面，如在图3中提供的用于提供用于保护个人内容的内容保护系统的方法的一个实施方式可以包括在操作100处接收被提交以供包括在内容保护系统中的个人内容的指示，以及在操作110处至少部分地基于与个人内容所源自的来源设备相关联的标记来确定个人内容向内容保护系统的准入资格。

[0050] 在某些实施方式中，该方法可以包括另外的可选操作，其示例在图3中用虚线示出。在各种备选实施方式中可以按照任何顺序和/或相互结合地执行可选操作。因此，例如，该方法还可以包括在操作120处支持准许个人内容进入内容保护系统并且与商业内容分开维护个人内容。附加地或者备选地，该方法可以包括在操作130处支持对向与提交个人内容以供包括在内容保护系统中的用户的经授权域相关联的设备的准入的个人内容的无限制移动和复制。

[0051] 在某些实施方式中，可以如下所述对以上操作中的某些操作进行修改或者进一步扩大。应当领会，以下的每个修改或者扩大可以单独地或者结合在此描述的特征中的任何其他特征而与以上操作一起被包括。在此方面，例如，确定个人内容的准入资格可以包括确定个人内容是否包括限定针对不与提交个人内容以供包括在内容保护系统中的用户的经授权域相关联的设备不允许对个人内容的无限制复制的使用状态。在某些情况中，确定个人内容的准入资格可以包括确定个人内容是否包括指示来源设备的水印或者基于关于个人内容是否包括与已知商业内容相关联的数字指纹的确定对准入资格进行确定。

[0052] 在示例性实施方式中，用于执行以上图3的方法的装置可以包括配置用于执行以上描述的操作(100-130)中的某些或者每个操作的处理器(例如处理器70)。该处理器可以例如配置用于通过执行硬件实现的逻辑功能、执行存储的指令或者执行用于执行每个操作(100-130)的算法而执行操作(100-130)。备选地，该装置可以包括用于执行以上描述的每个操作的装置。在此方面，根据示例实施方式，用于执行操作100-130的装置的示例可以包括例如处理器70、内容筛选器78和/或由处理器70执行以处理如以上描述的信息的算法。

[0053] 在此阐明的本发明的多种修改以及其他实施方式将为本发明所属于的领域中获益于上述描述以及相关联的附图中所呈现的教示的技术人员所知晓。因此，应当理解，本发明并不限于所公开的特定实施方式，并且上述修改和其他实施方式意在被包括在所附带的权利要求的范围中。此外，虽然上述描述以及相关联的附图在元件和/或功能的某些示例性组合的上下文中描述了示例性实施方式，但应当领会的是，备选实施方式可以提供元件和/或功能的不同组合而不会背离所附带的权利要求的范围。在此方面，例如，与以上详细描述的所不同的元件和/或功能的不同组合也预计可以在某些附带的权利要求中阐明。虽然在此使用了特定的术语，但它们仅仅在通用和描述性的意义中使用，并且并非意在限制。

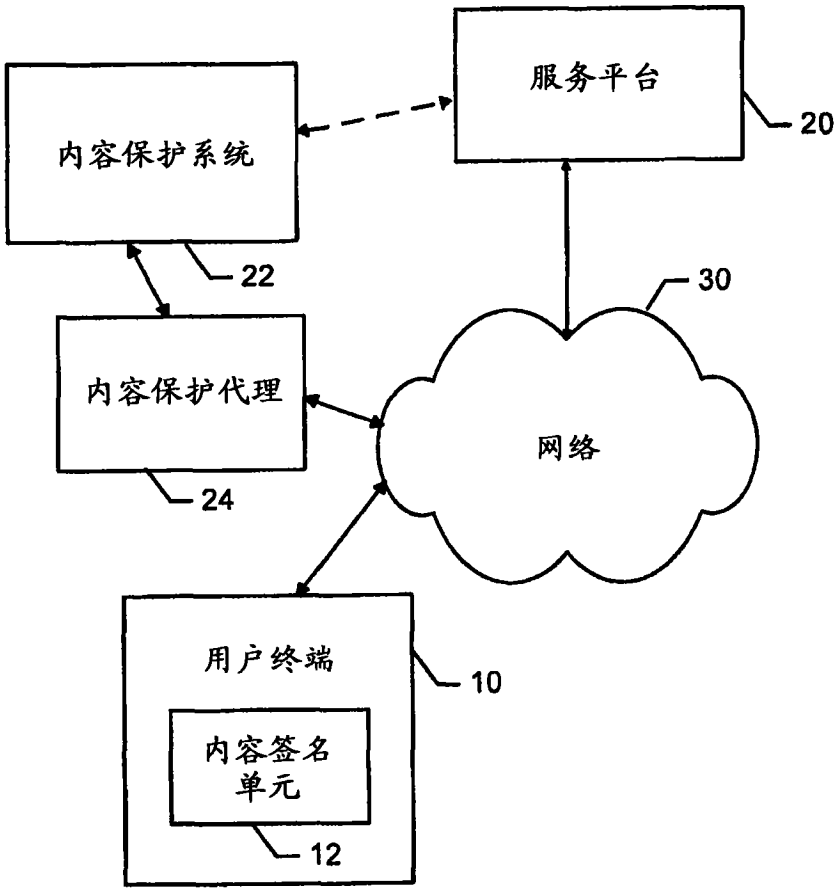


图1

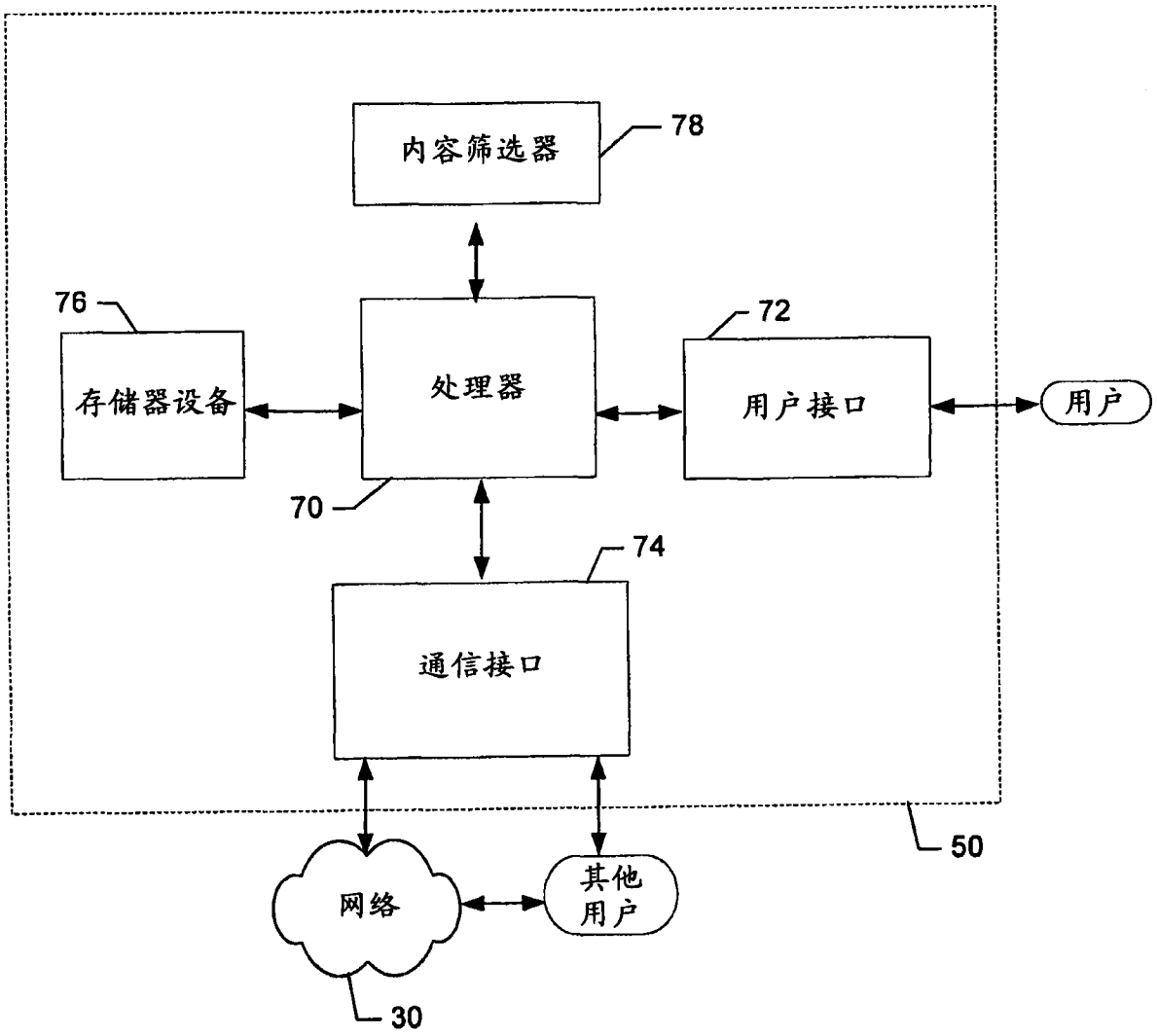


图2

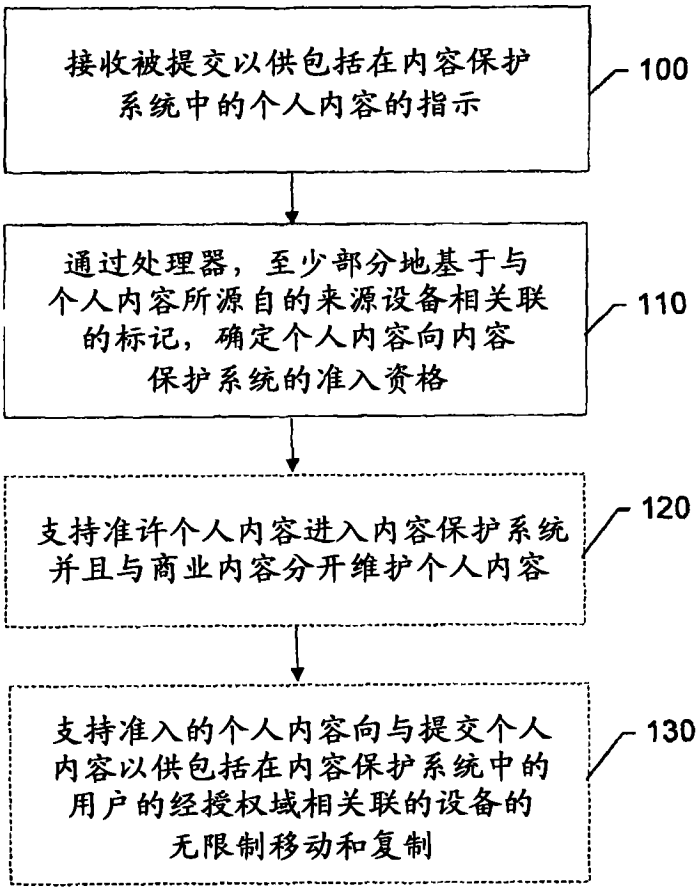

接收被提交以供包括在内容保护系统中的个人内容的指示
100
通过处理器，至少部分地基于与个人内容所源自的来源设备相关联的标记，确定个人内容向内容保护系统的准入资格
110
支持准许个人内容进入内容保护系统并且与商业内容分开维护个人内容
120
支持准入的个人内容向与提交个人内容以供包括在内容保护系统中的用户的经授权域相关联的设备的无限制移动和复制
130

图3